Decoding Quasi-Cyclic codes is NP-complete

Ernesto Dominguez Fiallo
Pablo Freyre Arrozarena
Luis Ramiro Piñeiro

Institute of Cryptography
Havana University

Abstract

We prove that the problem of decoding a Quasi-Cyclic (QC) code is NP-hard, and the corresponding decision problem is NP-complete. Our proof is based on a new characterization of quasi-cyclic codes closely related to linear random codes. We also discuss the cryptographic significance of this result.

1 Introduction

Coding Theory deals with the problem of detecting and correcting transmission errors caused by noise on the channel. The mathematical theory of the underlying principles started in 1948, when Shannon gave a formal description of a communication system and introduced a theory about the concept of information, including a measure for the amount of information in a message [27]. The relevance for cryptography of the Coding Theory began when Robert J. McEliece proposed a public key cryptosystem [22] that based its security on the NP-completeness of the Decisional Syndrome Decoding Problem (D-SDP) and Decisional Codeword Finding Problem (D-CFP) [7]. The McEliece cryptosystem originally uses Goppa codes [16, 17], so being rigorous, the security of the scheme is based on the complexity of the Goppa Bounded Decoding Problem (GBDP), whose associated decision problem has been shown to be NP-complete [13].

Currently, due to the large sizes of the public key of the original McEliece cryptosystem, other families of codes are used in order to find more compact mathematical representations of the keys, thus allowing their size to be reduced. However, these variants are built on

families of codes, mostly linear, in which it cannot be stated that the underlying computational problem is NP-hard. This constitutes an essential element in the theoretical security evaluation of post-quantum cryptographic schemes in general, and in particular, those based on codes. We refer the reader to papers [11, 24, 9, 8] to see the historical evolution and variants of the McEliece cryptosystem.

Among the code-based algorithms shortlisted for the NIST Post-Quantum contest [2], BIKE [23] and HQC [1] are based on Quasi-Cyclic (QC) codes, but in very different ways. The underlying computationally difficult problem is a variant of SDP called Quasi-Cyclic Syndrome Decoding Problem (QC-SDP). In this paper our interest is focused on the computational complexity of this problem.

It is known that for some parameters, QC codes have some properties similar to random codes in terms of minimum weight and probability distribution of the syndrome [10, 14, 21, 15, 12]. These properties are desirable in code-based cryptography. On the other hand, although there is no general complexity result for QC-SDP, this problem is considered hard by the cryptographic community [26] and the best known algorithms to solve it are the same to solve the SDP with the only advantage that the computational cost is reduced by a constant factor [25, 19]. There is an attempt to show that the decisional variant of QC-SDP is NP-complete but it is only limited to a particular form of QC codes [6].

Our contribution. In this paper we prove that the QC-SDP is NP-hard, and the corresponding decision problem is NP-complete (Theorem 3). Our result confirms the assumption so far assumed as valid that it is a difficult problem. To demonstrate our result, we previously demonstrated another way of looking at the structure of QC codes (Theorems 1 and 2). This new characterization of QC codes is closely related to random codes and is the starting point to demonstrate our result. We also discuss the cryptographic significance of this result, especially about the NIST post-quantum contest finalist algorithms that are based on codes.

2 Preliminaries

Let $\mathbb{F}_q$ be the Galois field of order a prime power q and let $\mathbb{F}_q^n$ denote the n-dimensional vector space defined over $\mathbb{F}_q$.

Definition 1. *A $[n,k]_q$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n and dimension k ($n > k$) is a k-dimensional subspace of $\mathbb{F}_q^n$, which can be represented by two matrices; a $k \times n$ generator matrix G, such that $\mathcal{C} = \{mG,\ m \in$*

$\mathbb{F}_q^k\}$ *or by a* $(n-k) \times n$ *parity-check matrix* H*, such that* $\mathcal{C} = \{c \in \mathbb{F}_q^n,\ Hc^T = 0\}$*, where* $c \in \mathcal{C}$*.*

Definition 2. *Let* $x, y \in \mathcal{C}$*. The Hamming distance* $d(x, y)$ *from* x *to* y*, is the number of places at which* x *and* y *differ. The Hamming weight* $w(x)$ *of* x *is the number of nonzero coordinates in* x*; i.e.,* $w(x) = d(x, 0)$*, where* 0 *is the zero word. The minimum distance of* $\mathcal{C}$*, denoted by* $d_{\min}$*, is* $d_{\min}(\mathcal{C}) = \min\{d(x, y) : x \neq y\}$*.*

If $\mathcal{C}$ has minimum distance $d_{\min}$, then is an exactly $t = \lfloor (d_{\min} - 1)/2 \rfloor$-error-correcting code.

Definition 3. *Let* $\mathcal{C}$ *be an* $[n, k]_q$ *linear code and let* H *be a parity-check matrix for* $\mathcal{C}$*. For any* $e \in \mathbb{F}_q^n$*, the syndrome* s *of* e *is the vector* $s = He^T \in \mathbb{F}_q^{n-k}$*.*

For any $s \in \mathbb{F}_q^{n-k}$ and parity-check matrix H, the set of vectors of $\mathbb{F}_q^n$ with syndrome s is denoted by $S_H^{-1}(s) = \{e \in \mathbb{F}_q^n : s = He^T\}$. By definition, $S_H^{-1}(0) = \mathcal{C}$ for any parity-check matrix H of $\mathcal{C}$. The vector space $\mathbb{F}_q^n/\mathcal{C}$ consist of all cosets $a + \mathcal{C} = \{a + c : c \in \mathcal{C}\}$ with $a \in \mathbb{F}_q^n$. There are exactly q^{n-k} different cosets, each coset contain q^k vectors, and form a partition of $\mathbb{F}_q^n$.

Definition 4. *[28] A Quasi-Cyclic (QC) code of index* n_0 *is a linear code with dimension* $k = p \cdot k_0$*, length* $n = p \cdot n_0$ *and have the property that each cyclic shift of a codeword by* n_0 *symbols yields another valid codeword.*

Given a vector $y \in \mathbb{F}_q^n$ and its syndrome $s = Hy^T$, decoding consists in find a codeword $c \in \mathcal{C}$ closest to y for the Hamming distance ($d(y, c) \leq t$) or find an error vector $e \in y + \mathcal{C}$ such that $w(e) \leq t$. In terms of algorithmic complexity, the corresponding decision problems are as follows:

Definition 5 (**Decisional Syndrome Decoding Problem (D-SDP)**)**.** *Given a random matrix* H*, a syndrome* s *and an integer* $t > 0$*, determine if exist a vector* e*, with* $w(e) \leq t$*, such that* $s = He^T$*.*

Definition 6 (**Decisional Codeword Finding Problem (D-CFP)**)**.** *Given a random matrix* H *and an integer* $t > 0$*, determine if exist a vector* e*, with* $w(e) \leq t$*, such that* $He^T = 0$*.*

The two decisional problems were proven to be NP-complete for the case of binary linear codes by Berlekamp et al. [7]. Barg generalized this proof to an arbitrary finite field [5] and finally, the NP-completeness proof has been generalized to arbitrary finite rings endowed with an additive weight [29].

The computational complexity theory states that any decision problem belonging to the NP-complete class has a search-to-decision reduction [3]. This states that the difficulty of SDP and CFP are as hard as an NP-complete problem. Although only decisional problems belong to the NP-complete class, in a commonly accepted abuse of language, it is said that SDP and CFP are NP-complete.

In the case of QC codes, the definition of the Quasi-Cyclic Syndrome Decoding Problem (QC-SDP) is as follows.

Definition 7. ***[Quasi-Cyclic Syndrome Decoding Problem (QC-SDP)]*** *Given a parity-check matrix H of a QC code, a syndrome s and an integer $t > 0$, find a vector e, with $w(e) \leq t$, such that $s = He^T$.*

3 NP-completeness of decoding QC codes

In this section it is shown that the QC-SDP is NP-complete. First, the QC codes are characterized by a representation of their parity-check matrix. This representation makes it possible to describe all QC codes through a close relationship with random codes. Then, using the parity-check matrix given by the previous representation, the NP-completeness is proved.

Usually the parity-check matrix of a QC code with length $n = p \cdot n_0$ and dimension $k = p \cdot (n_0 - r_0)$ is seen as follows

$$\begin{pmatrix} H^c_{00} & H^c_{01} & \dots & H_{0(n_0-1)} \\ H^c_{10} & H^c_{11} & \dots & H^c_{1(n_0-1)} \\ \vdots & \vdots & \ddots & \vdots \\ H^c_{(r_0-1)0} & H^c_{(r_0-1)1} & \dots & H^c_{(r_0-1)(n_0-1)} \end{pmatrix}$$

where each matrix H^c_{ij} with $0 \leq i \leq r_0 - 1$ and $0 \leq j \leq n_0 - 1$, is a $p \times p$ circulant matrix, that is, a matrix of the form

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{p-1} \\ a_{p-1} & a_0 & \dots & a_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}$$

with $a_l \in \mathbb{F}_q, 0 \leq l \leq p - 1$. A circulant matrix is associated through an isomorphism to a polynomial in x with coefficients over $\mathbb{F}_q$ given by the elements of the first row of the matrix:

$$a(x) = \sum_{i=0}^{p-1} a_i x^i$$

Therefore, the standard operations of matrix addition and multiplication can be performed in the ring of polynomials $\mathbb{F}_q[x]/(x^p - 1)$. However, from Definition 4, we can see QC codes from another perspective, more related to random codes.

Theorem 1. *Let $H_i,\ 0 \leq i \leq p-1$ be p any matrices, where each H_i has size $r_0 \times n_0$. The parity-check matrix*

$$H = \begin{pmatrix} H_0 & H_1 & \dots & H_{p-1} \\ H_{p-1} & H_0 & \dots & H_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ H_1 & H_2 & \dots & H_0 \end{pmatrix} \tag{1}$$

define a QC code with length $n = p \cdot n_0$ and dimension $k = p \cdot (n_0 - r_0)$.

Proof. The matrix H has size $r \times n$, with $r = p \cdot r_0$ (p matrices with r_0 rows) and $n = p \cdot n_0$ (p matrices with n_0 columns). Because $r = n - k$, we have $k = n - r = p \cdot (n_0 - r_0)$.

Given a generic codeword c of length n, it can be seen as $c = (c_0, c_1, \dots, c_{p-1})$ where each $c_i,\ 0 \leq i \leq p-1$ has size n_0. By definition 1, we have $Hc^T = 0$, that is:

$$\begin{gathered} H_0 \cdot c_0^T + H_1 \cdot c_1^T + \cdots + H_{p-1} \cdot c_{p-1}^T = 0 \\ H_{p-1} \cdot c_0^T + H_0 \cdot c_1^T + \cdots + H_{p-2} \cdot c_{p-1}^T = 0 \\ \vdots \\ H_1 \cdot c_0^T + H_2 \cdot c_1^T + \cdots + H_0 \cdot c_{p-1}^T = 0 \end{gathered}$$

Denoting by $c^{(x)},\ 1 \leq x \leq p-1$, the right cyclic shift of c in $x \cdot n_0$ positions and from the definition of QC code, we have that $c^{(x)}$ is a codeword too. Therefore, the equations

$$H \cdot \left(c^{(x)}\right)^T = 0,\ 1 \leq x \leq p-1 \tag{2}$$

must be satisfied. The equations $H \cdot \left(c^{(1)}\right)^T$ are

$$\begin{gathered} H_0 \cdot c_{p-1}^T + H_1 \cdot c_0^T + \cdots + H_{p-1} \cdot c_{p-2}^T \\ H_{p-1} \cdot c_{p-1}^T + H_0 \cdot c_0^T + \cdots + H_{p-2} \cdot c_{p-2}^T \\ \vdots \\ H_1 \cdot c_{p-1}^T + H_2 \cdot c_0^T + \cdots + H_0 \cdot c_{p-2}^T \end{gathered}$$

where the following pattern is observed:

- Equation 1 of $H \cdot \left(c^{(1)}\right)^T$ is the equation p of $Hc^T = 0$.
- Equation 2 of $H \cdot \left(c^{(1)}\right)^T$ is the equation 1 of $Hc^T = 0$, and so on.

That is, all the equations of $H \cdot \left(c^{(1)}\right)^T$ coincide with an equation of $Hc^T = 0$, therefore, it is satisfied that $H \cdot \left(c^{(1)}\right)^T = 0$. Let us now consider the equations $H \cdot \left(c^{(2)}\right)^T$

$$H_0 \cdot c_{p-2}^T + H_1 \cdot c_{p-1}^T + \cdots + H_{p-1} \cdot c_{p-3}^T$$

$$H_{p-1} \cdot c_{p-2}^T + H_0 \cdot c_{p-1}^T + \cdots + H_{p-2} \cdot c_{p-3}^T$$

$$\vdots$$

$$H_1 \cdot c_{p-2}^T + H_2 \cdot c_{p-1}^T + \cdots + H_0 \cdot c_{p-3}^T$$

Similarly, the following pattern is observed:

- Equation 1 of $H \cdot \left(c^{(2)}\right)^T$ is the equation p of $H \cdot \left(c^{(1)}\right)^T = 0$.
- Equation 2 of $H \cdot \left(c^{(2)}\right)^T$ is the equation 1 of $H \cdot \left(c^{(1)}\right)^T = 0$, and so on.

All the equations of $H \cdot \left(c^{(2)}\right)^T$ coincide with an equation of $H \cdot \left(c^{(1)}\right)^T = 0$, therefore $H \cdot \left(c^{(2)}\right)^T = 0$. Applying the same reasoning for all x, $1 \leq x \leq p-1$ in $H \cdot \left(c^{(x)}\right)^T$, it can be seen that the general pattern is as follows:

- Equation 1 of $H \cdot \left(c^{(x)}\right)^T$ is the equation p of $H \cdot \left(c^{(x-1)}\right)^T$.
- Equation i, $2 \leq i \leq p$, of $H \cdot \left(c^{(x)}\right)^T$ is the equation $i-1$ of $H \cdot \left(c^{(x-1)}\right)^T$.

Therefore, the equations 2 are satisfied and the code is QC. ■

The converse of the previous theorem also holds.

Theorem 2. *If $\mathcal{C}$ is a QC code of length $n = p \cdot n_0$ and dimension $k = p \cdot (n_0 - r_0)$, then the matrix*

$$H = \begin{pmatrix} H_0 & H_1 & \dots & H_{p-1} \\ H_{p-1} & H_0 & \dots & H_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ H_1 & H_2 & \dots & H_0 \end{pmatrix}$$

is a parity-check matrix for $\mathcal{C}$, where each matrix H_i, $0 \leq i \leq p-1$ has size $r_0 \times n_0$.

Proof. Let H' be a parity-check matrix of a QC code of length $n = p \cdot n_0$ and dimension $k = p \cdot (n_0 - r_0)$. Then H' can be written as follows

$$H' = \begin{pmatrix} H_{00} & H_{01} & \dots & H_{0(p-1)} \\ H_{10} & H_{11} & \dots & H_{1(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ H_{(p-1)0} & H_{(p-1)1} & \dots & H_{(p-1)(p-1)} \end{pmatrix}$$

where each matrix $H_{ij},\ 0 \leq i, j \leq p-1$ has size $r_0 \times n_0$. Since $\mathcal{C}$ is a QC code, for any codeword $c = (c_0, c_1, \dots, c_{p-1})$, the equalities

$$H' \cdot \left(c^{(x)}\right)^T = 0,\ 1 \leq x \leq p-1$$

are satisfied. Note that the equation 1 in $H' \cdot c^T = 0$ is the same as equation 2 in $H' \cdot \left(c^{(1)}\right)^T = 0$. Then is satisfied:

$$H_{00} = H_{11}$$

$$H_{01} = H_{12}$$

$$H_{02} = H_{13}$$

$$\vdots$$

$$H_{0(p-1)} = H_{10}$$

Similarly, we can consider the equation 3 in $H' \cdot \left(c^{(2)}\right)^T = 0$ and equation 4 in $H' \cdot \left(c^{(3)}\right)^T = 0$. This reasoning is extended to consider the equation p in $H' \cdot \left(c^{(p-1)}\right)^T = 0$ and it is obtained that

$$H_{00} = H_{11} = H_{22} = \dots = H_{(p-1)(p-1)}$$

$$H_{01} = H_{12} = H_{23} = \dots = H_{(p-1)0}$$

$$H_{02} = H_{13} = H_{24} = \dots = H_{(p-1)1}$$

$$\vdots$$

$$H_{0(p-1)} = H_{10} = H_{21} = \dots = H_{(p-1)(p-2)}$$

The previous equalities then mean that H' has the form (1), that is, $H' = H$. ■

Remark 1. *From theorems 1 and 2, it can be seen that if $n_0 = 1$, then the QC code matches a random code. More generally, any random code can be seen embedded in a QC code of greater index, length and dimension. However, it is clear that a QC code that has index $n_0 > 1$, does not match a random code of equal parameters due to the non-random structure of its parity-check matrix.*

From the previous theorems and from Remark 1, it is not difficult to deduce the proof of the following result.

Theorem 3. *The QC-SDP is NP-complete.*

Proof. The general idea of the proof is the following. Starting from an instance of the SDP, an instance of the QC-SDP is constructed in polynomial time and it is shown that if the latter is solved efficiently, then the instance of the former is necessarily solved efficiently.

Let (H, t, s) be an instance of the SDP and consider a QC code with length $n = p \cdot n_0$ and dimension $k = p \cdot (n_0 - r_0)$. The QC-SDP instance (H', t', s') is defined as follows. The matrix H' is

$$H' = \begin{pmatrix} H & H_1 & \dots & H_{p-1} \\ H_{p-1} & H & \dots & H_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ H_1 & H_2 & \dots & H \end{pmatrix}$$

where the matrices $H_i,\ 1 \leq i \leq p-1$ are any matrices of size $r_0 \times n_0$ randomly selected. Let $x \in \mathbb{F}_q^n$ be any vector. Because $n = p \cdot n_0$, x can be seen as $x = (x_0, x_1, \dots, x_{p-1})$ where each $x_i,\ 0 \leq i \leq p-1$ has length n_0. The value of t' is taken as $t + l$, with $l = \sum_{i=1}^{p-1} w(x_i)$. The syndrome s' is defined as $s' = (s + s_0, s_1, \dots, s_{p-1})$ where

$$H_1 \cdot x_1^T + \dots + H_{p-1} \cdot x_{p-1}^T = s_0$$

$$H_{p-1} \cdot x_0^T + H \cdot x_1^T + \dots + H_{p-2} \cdot x_{p-1}^T = s_1$$

$$\vdots$$

$$H_1 \cdot x_0^T + H_2 \cdot x_1^T + \dots + H \cdot x_{p-1}^T = s_{p-1}$$

and each $s_i,\ 0 \leq i \leq p-1$ has length r_0.

Let $\mathcal{A}$ be an algorithm capable of solving the instance (H', t', s') of the QC-SDP. This means that through $\mathcal{A}$, we can find a vector $e' = (e_1, e_2, \dots, e_n) \in \mathbb{F}_q^n$ with $w(e') \leq t'$ such that

$$H' \cdot e'^T = s'$$

The vector e' can be seen as $e' = (e_0, e_1, \dots, e_{p-1})$ where each $e_i,\ 0 \leq i \leq p-1$ has length n_0 and $\sum_{i=1}^{p-1} w(e_i) = l$. Thus, we have that $H' \cdot e'^T = s'$ is

$$H \cdot e_0^T + H_1 \cdot e_1^T + \dots + H_{p-1} \cdot e_{p-1}^T = s + s_0$$

$$H_{p-1} \cdot e_0^T + H \cdot e_1^T + \dots + H_{p-2} \cdot e_{p-1}^T = s_1$$

$$\vdots$$

$$H_1 \cdot e_0^T + H_2 \cdot e_1^T + \cdots + H \cdot e_{p-1}^T = s_{p-1}$$

By definition, $s_0 = \sum_{i=1}^{p-1} H_i \cdot e_i^T$. Substituting s_0 in the first of the above equations we get

$$H \cdot e_0^T = s$$

Since $w(e) \leq t'$, we have that $w(e_0) \leq t' - l = t$. Therefore, e_0 is a solution of the instance of the SDP. In this way, a solution of the QC-SDP allows to find in polynomial time, a solution of an instance of the SDP.

3.1 Cryptographic significance.

The proof that the QC-SDP is NP-complete means that it is difficult in the worst case. Although this says nothing of the average case complexity, maybe it does not fall into an easy instance (see discussion of [20, 18] and section 3.2 of [4]).

The NIST submission BIKE combines QC codes of index 2 with MDPC codes. In this case, we are in the presence of a particular case of the QC-SDP problem, that is, when $n_0 = 2$. However, since QC-MDPC codes constitute a subfamily of QC codes, our result does not affirm that BIKE bases its security on an NP-complete problem, but it reinforces that idea due to the possible closeness of the MDPC codes to the random ones.

On the other hand, HQC is based on the quasi-cyclic concatenation of the Reed-Muller and Reed-Solomon codes. Since these families of codes are not random, our result finds no applicability in HQC.

4 Conclusion

In this paper we have proved that the QC-SDP is NP-hard and its corresponding decision variant is NP-complete. This problem was considered difficult but until now no proof of such a statement was known. Our result is directly related to theoretical security analyzes of code-based post-quantum cryptographic schemes, in particular, BIKE and HQC, which are finalists in the NIST Post-Quantum Asymmetric Standards Contest.

In the case of BIKE, our result reinforces the hypothesis that its security is based on an NP-complete problem. In the case of HQC, the same cannot be stated due to the families of codes that it concatenates in a quasi-cyclic structure.

References

[1] Aguilar-Melchor, C., Blazy, O., Deneuville, J.-C., Gaborit, P., and Zémor, G. Efficient encryption from random quasi-cyclic codes. *IEEE Transactions on Information Theory 64*, 5 (2018), 3927–3943.

[2] Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., and et. al. Status report on the third round of the nist post-quantum cryptography standardization process. *US Department of Commerce, NIST* (2022).

[3] Arora, S., and Barak, B. *Computational complexity: a modern approach*. Cambridge University Press, Cambridge, 2009.

[4] Augot, D., Finiasz, M., and Sendrier, N. A family of fast syndrome based cryptographic hash functions. In *Mycrypt* (2005), vol. 3715, Springer, pp. 64–83.

[5] Barg, S. Some new np-complete coding problems. *Problemy Peredachi Informatsii 30*, 3 (1994), 23–28.

[6] Berger, T. P., Cayrel, P.-L., Gaborit, P., and Otmani, A. Reducing key length of the mceliece cryptosystem. In *Progress in Cryptology–AFRICACRYPT 2009: Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009. Proceedings 2* (2009), Springer, pp. 77–97.

[7] Berlekamp, E., McEliece, R., and Van Tilborg, H. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory 24*, 3 (1978), 384–386.

[8] Bolkema, J., Gluesing-Luerssen, H., Kelley, C. A., Lauter, K. E., Malmskog, B., and Rosenthal, J. Variations of the mceliece cryptosystem. In *Algebraic Geometry for Coding Theory and Cryptography: IPAM, Los Angeles, CA, February 2016* (2017), Springer, pp. 129–150.

[9] Bucerzan, D., Dragoi, V., and Kalachi, H. T. Evolution of the mceliece public key encryption scheme. In *Innovative Security Solutions for Information Technology and Communications: 10th International Conference, SecITC 2017, Bucharest, Romania, June 8–9, 2017, Revised Selected Papers 10* (2017), Springer, pp. 129–149.

[10] Chen, C., Peterson, W. W., and Weldon Jr, E. Some results on quasi-cyclic codes. *Information and Control 15*, 5 (1969), 407–423.

[11] Engelbert, D., Overbeck, R., and Schmidt, A. A summary of mceliece-type cryptosystems and their security. *Journal of Mathematical Cryptology 1*, 2 (2007), 151–199.

[12] Fiallo, E. D. A digital signature scheme mcfs^qc-ldpc based on qc-ldpc codes. *Mathematical Aspects of Cryptography 12*, 4 (2021), 99–113.

[13] Finiasz, M. Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie à clef publique. *These de doctorat, École Polytechnique* (2004).

[14] Finiasz, M., Gaborit, P., and Sendrier, N. Improved fast syndrome based cryptographic hash functions. In *Proceedings of ECRYPT Hash Workshop* (2007), vol. 2007, Citeseer, p. 155.

[15] Gaborit, P., and Zemor, G. Asymptotic improvement of the gilbert–varshamov bound for linear codes. *IEEE Transactions on Information Theory 54*, 9 (2008), 3865–3872.

[16] Goppa, V. D. A new class of linear correcting codes. *Problemy Peredachi Informatsii 6*, 3 (1970), 24–30.

[17] Goppa, V. D. A rational representation of codes and (l, g)-codes. *Problemy Peredachi Informatsii 7*, 3 (1971), 41–49.

[18] Gurevich, Y. Average case completeness. *Journal of Computer and System Sciences 42*, 3 (1991), 346–398.

[19] Hauteville, A., and Tillich, J.-P. New algorithms for decoding in the rank metric and an attack on the lrpc cryptosystem. In *2015 IEEE International Symposium on Information Theory (ISIT)* (2015), IEEE, pp. 2747–2751.

[20] Levin, L. A. Average case complete problems. *SIAM Journal on Computing 15*, 1 (1986), 285–286.

[21] MacWilliams, F. J., and Sloane, N. J. A. *The theory of error-correcting codes*. Elsevier, North Holland, 1977.

[22] McEliece, R. J. A public-key cryptosystem based on algebraic. *Coding Thv 4244* (1978), 114–116.

[23] Misoczki, R., Tillich, J.-P., Sendrier, N., and Barreto, P. S. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *2013 IEEE international symposium on information theory* (2013), IEEE, pp. 2069–2073.

[24] Repka, M., and Zajac, P. Overview of the mceliece cryptosystem and its security. *Tatra Mountains Mathematical Publications 60*, 1 (2014), 57–83.

[25] Sendrier, N. Decoding one out of many. In *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4* (2011), Springer, pp. 51–67.

[26] Sendrier, N. Code-based cryptography: State of the art and perspectives. *IEEE Security & Privacy 15*, 4 (2017), 44–50.

[27] Shannon, C. E. A mathematical theory of communication. *The Bell system technical journal 27*, 3 (1948), 379–423.

[28] Townsend, R., and Weldon, E. Self-orthogonal quasi-cyclic codes. *IEEE Transactions on Information Theory 13*, 2 (1967), 183–195.

[29] Weger, V., Khathuria, K., Horlemann, A.-L., Battaglioni, M., Santini, P., and Persichetti, E. On the hardness of the lee syndrome decoding problem. *arXiv preprint arXiv:2002.12785* (2020).